Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report
for 30 September 2003

Daily Overview

- The Associated Press reports Amtrak has asked the U.S. District Court for the District of Columbia to halt a union walkout that could affect intercity passenger service as well as commuter trains in some major cities. (See item 6)

- Reuters reports an outbreak of malaria in Florida this past summer is the first U.S. outbreak since 1986 to have started with just one person. (See item 17)

- Reuters reports computer experts have cautioned that security holes in Microsoft's Internet Explorer are being exploited by hackers. (See item 25)

- The Advertiser reports Yemeni authorities have alerted the U.S. to a potential new terrorist threat against foreign targets in Yemen. (See item 26)

DHS/IAIP Update *Fast Jump*

Production Industries: **Energy**; **Chemical**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information and Telecommunications**; **Internet Alert Dashboard**

Other: **General**; **DHS/IAIP Web Information**

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – http://esisac.com]

1. *September 29, Reuters* — **Italy gets power back after massive blackout.** Italy got its power back fully on Monday, September 29, after a collapse of the electricity grid plunged millions into darkness on Sunday, September 28. As engineers nursed the network back to capacity, politicians said **Sunday's sudden outage had given Italy a wake–up call to make economic**

reforms, including measures to boost power output and cut reliance on electricity imports. Tens of thousands of rail passengers were stranded and hundreds of people had to be rescued from elevators as the grid went down, just four seconds after an interruption in French and Swiss power supplies at around 3:20 a.m. on Sunday. **The cause of the blackout appeared to have been a tree which was uprooted by strong wind and hit a Swiss transmission line taking power into Italy. That could have caused over–capacity on French lines to Italy, resulting in a domino–like collapse. Italy relies on imports for 17 percent of its power, most of it from France, which has plentiful nuclear supplies. Italy banned nuclear power after a referendum in 1987.**
Source: http://www.reuters.com/newsArticle.jhtml;jsessionid=KUCHVDSV
T3VNWCRBAELCFFA?type=worldNews&storyID=3525317

2. *September 29, Reuters* — **Vermont Yankee nuke shut down due to leak. Entergy Nuclear said on Monday, September 29, it fixed a small leak in the reactor cooling system at the 510 megawatt Vermont Yankee nuclear unit in Vermont and was preparing to restart the unit. The leak, caused by a problem with the packing in a valve on the reactor head vent, did not pose any danger to the health and safety of the public.** "It was completely contained by the containment system. In the vent is a small two inch line. We repacked it and are preparing to return the unit to service," said Brian Cosgrove, a spokesperson for the plant. The unit was shut down on Saturday, September 27, because of an "unidentified primary containment leakage" of greater than two gallons per minute. The Vermont Yankee station is located five miles south of Brattleboro, VT.
Source: http://biz.yahoo.com/rm/030929/utilities_entergy_vermontyank ee_2.html

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *September 29, Associated Press* — **Liberian exit. American troops have started pulling out of the peacekeeping mission in Liberia, defense officials said Monday, September 29.** The amphibious landing dock USS Carter Hall and amphibious transport dock USS Nashville started moving north in the Atlantic during the weekend and were likely to make a maintenance stop in Europe before heading home, according to defense officials. That leaves the USS Iwo Jima amphibious assault ships off Liberia's shore with some 2,600 sailors and Marines aboard, and about 100 other troops in Liberia, the vast majority providing security for the U.S. Embassy in the capital of Monrovia. African leaders and others had asked the United States in early summer to send troops to lead a peacekeeping force in the country ravaged by years of conflict. But U.S. officials stressed as they debated the mission in June and July that they wanted only minimal involvement. As troops deployed in August, President Bush said they would leave by October 1. **Meanwhile, some 3,250 U.S. troops serving in the Nigerian–led West African stabilization force will don blue helmets when the United Nations takes over peacekeeping**

this week, UN officials said Sunday.
Source: http://www.kansascity.com/mld/kansascity/news/breaking_news/ 6889568.htm

4. *September 29, PostNewsweek Tech Media* — **Work refined on Air Force C2 subsystem.** The Air Force has chosen three contractors to compete to develop the Battle Management Command and Control (BMC2) subsystem for the agency's new $60 billion E−10A Multisensor C2 aircraft. The E−10A will provide the Air Force with next−generation cruise missile defense and airborne ground surveillance and targeting capabilities. The BMC2 subsystem must collect, integrate and distribute sensor data collected by the aircraft's Multi−Platform Radar Technology Insertion Program radar and other Air Force C2 sensors.
Source: http://www.washingtontechnology.com/news/1_1/daily_news/2180 7−1.html

[Return to top]

Banking and Finance Sector

Nothing to report.
[Return to top]

Transportation Sector

5. *September 29, Government Technology* — **Ohio airport adopts biometric system. Demonstrating its commitment to security and serving as an example for other airports to follow, Toledo Express Airport, Toledo, OH, unveiled its new biometric security system, which accurately verifies the identity of an individual by the unique physical characteristics of his or her hand.** With the new system, Toledo Express is the second airport in the United States and the first in the Midwest to completely control access to its tarmac and other sensitive areas using biometric technologies. **Toledo Express is among a group of airports globally that has begun to employ HandReaders to monitor employees, who often have access to sensitive areas of an airport where employee and passenger security could be compromised.** In addition to Toledo Express, San Francisco International Airport and Ben Gurion Airport in Israel use HandReaders to monitor employees for greater security.
Source: http://www.govtech.net/news/news.php?id=2003.09.29−70006

6. *September 29, Associated Press* — **Amtrak asks court to halt walkout.** Amtrak asked the U.S. District Court for the District of Columbia on Monday to halt a union walkout that could affect intercity passenger service as well as commuter trains in some major cities. **Amtrak President David Gunn has told the unions that the threatened strike would be "ill−advised and illegal."** Charles Moneypenny, director of the railroad division of the Transport Workers Union of America, said the unions will contest a restraining order. Another union, Transportation Communications Union, which represents about half of Amtrak's unionized employees, said last week it won't participate in the stoppage. Amtrak asked for $1.8 billion in federal subsidies in 2004. President Bush proposed half that amount as a way to force the railroad to restructure itself. **The House agreed this month to give the railway $900 million next year. The Senate is proposing $1.346 billion.**
Source: http://www.cnn.com/2003/TRAVEL/09/29/bi.amtrak.walkout.ap/

7. *September 29, Dallas–Ft. Worth Star Telegram* — **U.S. to resume airline security tax.** Travelers can expect a bump up in airfares at the end of the month, when a summer holiday from an airline security tax ends. **On October 1, the government is scheduled to reinstate a $2.50 per connection tax on all airfares, which is designed to cover security costs. Congress temporarily lifted the tax on June 1, as part of its $3.1 billion relief package for the airline industry that was approved in April. Analysts say the carriers aren't likely to reduce fares to absorb the tax when it returns. That means customers will pay the security charge on top of the ticket price.** "It's going to be an additional fare hike for the consumers, and the airlines will be able to blame the government," said Tom Parsons, chief executive of Bestfares, an Arlington–based travel service that monitors airfares. Officials with American declined to comment on the tax, and how they would respond to its return. **The tax is scheduled to return as several airlines launch fall and winter fare sales, in the hopes of spurring traffic during a traditionally slow period.**
Source: http://www.dfw.com/mld/dfw/business/6842973.htm

[Return to top]

Postal and Shipping Sector

8. *September 29, eWeek* — **UPS delivers technology. Bankrolled by a $1 billion IT budget, United Parcel Service of America Inc. (UPS) is using technology to increase efficiency in package delivery, while it moves beyond that narrow discipline to become a broad supply chain integrator. UPS announced last week a suite of Package Flow Technologies, including software, hardware and new processes.** The software alone commanded a $30 million investment, both in new code and in integration with existing technology. The software includes such capabilities as allowing customers to make in–transit changes to delivery instructions. The technology enables UPS to automate delivery route planning to optimize timely delivery and reduce the route length. Previously, drivers had to map their own routes, a sometimes–difficult, time–consuming process. The automated route–planning system, called Package Flow, will reduce the distance driven by delivery trucks by more than 100 million miles annually, saving 14 million gallons of fuel, UPS officials estimate. **The software is now in 50 UPS package–handling centers and will be in 80 by year's end, officials said. It promises to be in 1,000 locations by 2005, they said.**
Source: http://www.eweek.com/article2/0,4149,1304156,00.asp

[Return to top]

Agriculture Sector

9. *September 28, The Daily Sentinel (CO)* — **Colorado lawmaker to back pharmaceutical crops in state. A Colorado state lawmaker will endorse the introduction of pharmaceutical crops into the state, provided that strict regulations are enacted first.** "I feel confident that we have enough information to move forward on this," Rep. Ray Rose, R–Montrose, said. Pharmaceutical companies are eyeing Colorado farms as suitable locations to grow genetically engineered corn. The plants yield compounds used in medicines. Rose traveled to France this

month to observe a company growing pharmaceutical crops, which convinced him that the process is safe, but showed him where U.S. regulations fall short. **Rose wants strict state regulations on par with French regulations before next year's growing season. "Holes" exist in regulations of pharmaceutical plants enforced by the U.S. Department of Agriculture and Federal Drug Administration, Rose said.** The state should enact regulations that provide "minimum safety standards," he said. Flexible guidelines to apply those regulations to individual crops are needed, he added.
Source: http://www.gjsentinel.com/news/newsfd/auto/feed/news/2003/09/28/1064724028.19830.8626.2646.html;COXnetJSessionID=13N7jxcAW1YJhFxgx80LcA1Y0DNK2JkHIPP6txilRKLLYkpJzoXO!−621130288?urac=n&urvf=10647832913200.5444454119922668

10. *September 28, Santa Cruz Sentinel (CA)* — **Agriculture industry watchful of terrorist acts. What started as a way to maintain quality control and protect consumers from food−borne illnesses for farmers like Ken Lewis has become a national model for food security against terrorism.** Lewis implemented a tracking system 15 years ago to ensure that the strawberries, lettuce and vegetables he grows arrive to market fresh and free of pesticides. But **with the concern of terrorism, the system is being used to inform growers who have handled their produce.** Lewis can trace a strawberry from who picked it in the field to what supermarket it ends up in. "Quite frankly, we're vulnerable," said James Moseley, deputy secretary of the U.S. Department of Agriculture. **Even the hint that a food supply has been compromised in one area could affect the national market,** according to Dave Moeller, Santa Cruz County agricultural commissioner. "It doesn't have to be a big bomb to have a dramatic economic effect," he said.
Source: http://www.santacruzsentinel.com/archive/2003/September/28/local/stories/03local.htm

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

11. *September 29, Sun−Sentinel (FL)* — **Business group pushes plan to rewrite Florida's water laws.** Some of Florida's most powerful business interests want Florida's water−rich areas to share their wealth. **In a call to rewrite Florida water laws, a group of advisers to Gov. Jeb Bush contend water is a state resource that should be transferred from areas of the state swimming with it to those that might not have enough.** The proposal, unveiled on Thursday by the Florida Council of 100, also calls for a statewide commission to better monitor the water supply and prevent future shortages that could damage the environment and development. "This state needs to get a grip on growth before we start tapping into taxpayers' scarce dollars right now to provide vast quantities of water for many millions of people that we're not necessarily stuck with at this point," said Linda Young, head of the Florida Clean Water Network. But

proponents warn that the state could need up to 2 billion gallons of extra water per day to deal with a population that is expected to hit 21.8 million by 2020. **Florida's problem is that 80 percent of its water is north of Interstate 4 while 80 percent of the consumption is south, said Clearwater developer Lee Arnold, who leads the council's 30–member water task force.**
Source: http://www.sun−sentinel.com/news/local/florida/sfl−fwater26s ep26,0,6834419.story?coll=sfla−news−florida

12. *September 29, Star−Ledger (NJ)* — **New Jersey too generous with water, critics say.** Despite last year's severe drought, the state is authorizing water usage faster than it has in years. **Last year the state gave out 152 water−allocation permits, which are licenses to take more than 100,000 gallons a day. Many go to golf courses, large commercial complexes, housing developments, and towns that want to grow.** Though it is difficult to gauge exactly how many gallons are being used, the increased number of permits has sparked concern among environmentalists, **who say the lesson of the drought was that New Jersey must be more diligent about conserving its water supply.** "Water allocation needs to get to the point where they're able to say no," said Richard Bizub, a groundwater geologist with the Pinelands Preservation Alliance. They worry about golf course runoff lacing water with herbicides and poisoning ecosystems. They point to increasing signs of water scarcity in recent years. **In Camden County, for example, a municipal well sucked the water out of a stream that was lined with endangered plants. In coastal areas, saltwater is intruding into aquifers because more fresh water is being sucked out of the ground.**
Source: http://www.nj.com/news/ledger/jersey/index.ssf?/base/news−4/ 106472470562590.xml

13. *September 28, KXMC News (ND)* — **Town water supply in question. Community leaders in Parshall, ND, want help making sure they can get water from Lake Sakakawea this winter.** Mayor Herb Zacher says that if the U.S. Army Corps of Engineers maintains the lake's level, Parshall will be all right. The lake has been about 1821 feet above sea level. Zacher says that if the lake drops to 1817 feet or less, they'll be in trouble. That's because **the city's water intake would be near the surface, and could be iced over this winter.** Parshall gets water from an intake about 10 miles west of town. Auditor Loren Hoffman says Parshall has a backup source −− but those wells give poor−quality water. Zacher says he's notified the North Dakota Division of Emergency Management about the situation. A spokesman says emergency officials are working on a meeting with the Corps of Engineers to discuss the problem.
Source: http://www.kxmc.com/news/local.asp?ID=2531

14. *September 28, The Kansas City Star* — **As rural water systems fail, locals worry −− and sometimes lay pipelines themselves.** In rural communities nationwide, water mains laid generations ago are cracking because of age, and cash−strapped towns can't afford to fix the extensive underground systems. **Repair, replacement or improvement could cost between $154 billion and $446 billion over the next 20 years, according to a U.S. Environmental Protection Agency study.** "Conditions in small communities are becoming increasingly desperate," says John Mori, executive director of the National Environmental Services Center at West Virginia University, a federally funded organization that provides technical assistance on small−town water, sewer and trash projects. **In some towns, residents are picking up shovels themselves to do the work – and save money.** When Corning, KS (population 170) learned it would cost $418,000 to replace 4.1 miles of frequently leaking pipes – or about $2,500 per

person – nearly 100 people volunteered to help. They offered to dig trenches and lay pipe, but also to cook food, baby–sit and run errands – enough labor to cut the cost in half.
Source: http://www.kansascity.com/mld/kansascity/news/breaking_news/ 6883786.htm

[Return to top]

Public Health Sector

15. *September 26, Associated Press* — **Technology may deter counterfeit drugs. Radio–tagged product codes that are gaining popularity for inventory control might also one day help keep counterfeit medicine out of the drug supply.** Drug makers and sellers are urging the Food and Drug Administration (FDA) to consider the new technology as it seeks safeguards against the growing threat of counterfeit medicine, said FDA pharmacy chief Tom McGinnis, who heads the agency's new anti–counterfeiting task force. **It's a still–evolving technology, so widespread use on prescription drugs is probably a few years away, McGinnis said.** Although, he expects some companies with drugs particularly vulnerable to counterfeiters will try it sooner. **Also drawing FDA attention is a program by Serono Inc. that tracks every box of a treatment for AIDS wasting, called Serostim, from factory to a network of pharmacies specially authorized to sell it.** Additionally, pharmacies must report that bar–coded tracking number to get reimbursement from certain third–party payers. **Serono started the program last fall, after a rash of Serostim counterfeits. No fakes have been detected since, Serono Vice President James Sapirstein said.** The FDA has investigated more than 20 counterfeiting cases a year since 2000, up from roughly five a year in the 1990s.
Source: http://www.boston.com/yourlife/health/diseases/articles/2003 /09/26/technology_may_deter_counterfeit_drugs/

16. *September 26, Reuters* — **Drug halts progress of 'Mad Cow Disease' in UK man.** An experimental treatment given to a Northern Irish teenager has halted the progress of brain damage caused by the human form of mad cow disease, medical experts studying his case said on Friday, September 26. **Jonathan Simms, 19, from Belfast, is the first person to have pentosan polysulphate (PPS) injected into his brain in an attempt to slow the damage caused by variant Creutzfeldt–Jakob Disease (vCJD). "Here we have a kid who had gone down and down and down, now he's put all the weight he had lost back on, his heart rate is back up to normal,"** said Stephen Dealler, a consultant microbiologist at the Royal Lancaster Infirmary in England. "It is one case, and you can't go round saying we have the answer, but it has justified large amounts of work to go ahead to find out what was really going on, to find out why the drug appeared to have such an effect and which way to go from here." **There is no cure for vCJD, which is fatal and has been linked to eating meat from cattle infected with Bovine Spongiform Encephalopathy (BSE), also known as mad cow disease.**
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=3515801

17. *September 26, Reuters* — **Source unclear for Florida malaria outbreak. An outbreak of malaria in Florida this past summer is the first U.S. outbreak since 1986 to have started with just one person, a new report indicates.** Strangely, this patient had no risk factors for the disease. **While most cases of malaria in the U.S. are imported, locally acquired cases continue to occur,** the authors note in the Morbidity and Mortality Weekly Report. Dr. J. M. Malecki, of Palm Beach County Health Department, and colleagues describe seven patients

diagnosed with malaria after hospital admission between July 24 and August 26. None had a history of malaria, recent blood transfusion, organ transplantation or IV drug use–all risk factors for malaria. The patients all lived within 10 miles of Palm Beach International Airport. However, of more than 400 mosquitoes trapped within one mile of patients' homes, none harbored the parasite that caused their type of malaria. Testing the parasites obtained from the patients revealed that all were the same strain. **According to an editorial note, "these results support the hypothesis that this cluster of cases was the result of...malaria originating from a single infected person."**
Source: http://www.reuters.com/newsArticle.jhtml?type=healthNews&sto ryID=3513455

[Return to top]

Government Sector

18. *September 29, thetimesherald.com* — **County should make the most of Ridge's visit. Homeland Security Secretary Tom Ridge is due in St. Clair County, Michigan, next month. The county is a significant security zone –– the Blue Water Bridge is a key link between the United States and Canada, one that is vital to U.S.–Canadian trade. Also, one of the largest volumes of hazardous materials in North America passes over the bridge each day. The St. Clair River rail tunnel is a vital international link, as well. It makes the county a leading hub for U.S.–Canadian train commerce.** And, there is Sarnia's Chemical Valley. One of the largest petrochemical manufacturing sites in North America, its concentration of production facilities along the St. Clair River's Canadian shore strengthen the case for treating St. Clair County as a top priority for security. **County leaders want a central dispatch system, one that would replace the three centers the sheriff department, Clay Township and Port Huron currently use.** This single service connecting all police, fire and other emergency responders makes perfect sense. Its $12.4 million price tag, though, is a bit daunting, without federal help.
Source: http://www.thetimesherald.com/news/stories/20030929/opinion/ 353522.html

19. *September 29, Government Technology* — **Graduate Degree in Homeland Security.** Current and future managers from all aspects of the public safety arena –– such as law enforcement, fire service, emergency management, public health –– may take advantage of a new program that lets them earn a master's degree in homeland security, paid for by federal funds. **Created by the Office for Domestic Preparedness, an agency of the U.S. Department of Homeland Security, and located at the Naval Postgraduate School in Monterey, CA, it focuses on creating the leaders of the future by teaching them the concepts, theories, and models applicable to homeland protection and defense. Program participants will learn about world politics and governments and how each handles terrorism, as well as the different types of terrorists and terrorism.** They will learn about the layers of infrastructure, including water, power, transportation, information technology, finance, and methods for determining the "critical nodes" and interdependencies of the infrastructure in their own localities. Other courses focus on the relationship between civil and military organizations; fear management; and asymmetrical warfare.
Source: http://www.govtech.net/news/news.php?id=2003.09.29–70002

[Return to top]

Emergency Services Sector

20. *September 29, WESH (Florida)* — **Federal grant means better communication in emergencies. In Orlando, Fl, the head of the region's Domestic Security Task Force announced a major boost to emergency communications Monday. Whether it's a homeland security threat or hurricane, communication in the nine–county region will be improved, Orange County Sheriff Kevin Beary said.** That's because of a $6 million federal grant. Each county currently has its own radio system and only two channels where emergency responders can intercommunicate. **First responders from Daytona Beach to Port St. Lucie will now have more direct communication with each other when seconds count.** Region 5, which includes Central Florida, is one of the first in the county to get this type of money. **It will take about a year to get all nine counties connected with five additional mutual–aid radio channels.**
Source: http://www.wesh.com/news/2518695/detail.html

21. *September 29, Union Tribune (San Diego)* — **Biometrics setbacks and successes.** Automated scanning of eyes, faces or fingerprints once promised to provide the keys and passwords of our high–tech future. **After 9/11, the emerging technology known as biometrics has taken on a new priority. There was much hope that computers could read the unique appearance of the tissue within the eye or the structure of a face to help keep terrorists out of the country, out of the airports.** Some of the most challenging uses – scanning a crowd and comparing faces against a database of suspects, for example – have been declared not ready for regular use. **Other, more proven applications need to be ready; Congress has mandated that biometric identifiers be encoded in all passports and visas issued after October 26, 2004, for foreigners entering the United States. At customs, a traveler will stand in front of a digital camera. A computer will read the encoded information in the passport and compare it with the digital image.** The Transportation Security Administration is also looking at biometrics as part of a "trusted traveler" program that would identify low–risk airline passengers and make it easier for them to clear security.
Source: http://www.signonsandiego.com/news/computing/personaltech/20 030929–9999_mz1b29biomet.html

22. *September 28, Augusta Chronicle* — **Railcar leak forces neighborhood evacuation. A railcar leaking ammonium nitrate forced about 30 residents to evacuate a Hartsville, SC, neighborhood on Sunday.** Darlington County Emergency Management Division spokesman Linwood Epps said people were evacuated within four blocks of a rail yard where the leaking rail car was discovered around 8:45 a.m. No injuries were reported. **Ammonium nitrate, a chemical used to make fertilizer, is corrosive. It is harmful if fumes are inhaled or if it comes into contact with skin, state Department of Health and Environmental Control spokesman Thom Berry said.** The car continued to leak Sunday evening, Berry said. A crew was on the way to begin cleaning up a pool of liquid about 100–feet wide that formed around the tank car. The 20,000 gallon car was full when it was shipped, Berry said. He did not know where the tank car was filled, where it began leaking or how much of the chemical was spilled. Epps said the car was leased by Trademark Nitrogen Corp. of Tampa, FL. Company officials were not immediately available Sunday to discuss the leak.
Source: http://www.augustachronicle.com/stories/092903/met_124–3785. shtml

23. *September 25, Expatica.com* — **Paris metro to rehearse chemical attack.** Paris police and rescue workers will stage a simulated chemical attack in the Invalides metro station sometime in October to test emergency response systems, police said Thursday. **The test exercise – similiar to one carried out in the London underground earlier this month, but on a smaller scale – will help emergency personnel practice quarantine, decontamination and rescue procedures. The Invalides metro station is located in the heart of the French capital near a host of ministries and embassies, including the French foreign ministry, and the gold–domed church that houses Napoleon Bonaparte's tomb. The station is also a hub for the French capital's regional express rail services.** Hundreds of British police and emergency workers participated in a major terror attack simulation in the heart of London's financial district on September 7, four days before the second anniversary of the September 11 attacks in the United States.
Source: http://www.expatica.com/france.asp?pad=278,313,&item_id=3454 9

[Return to top]

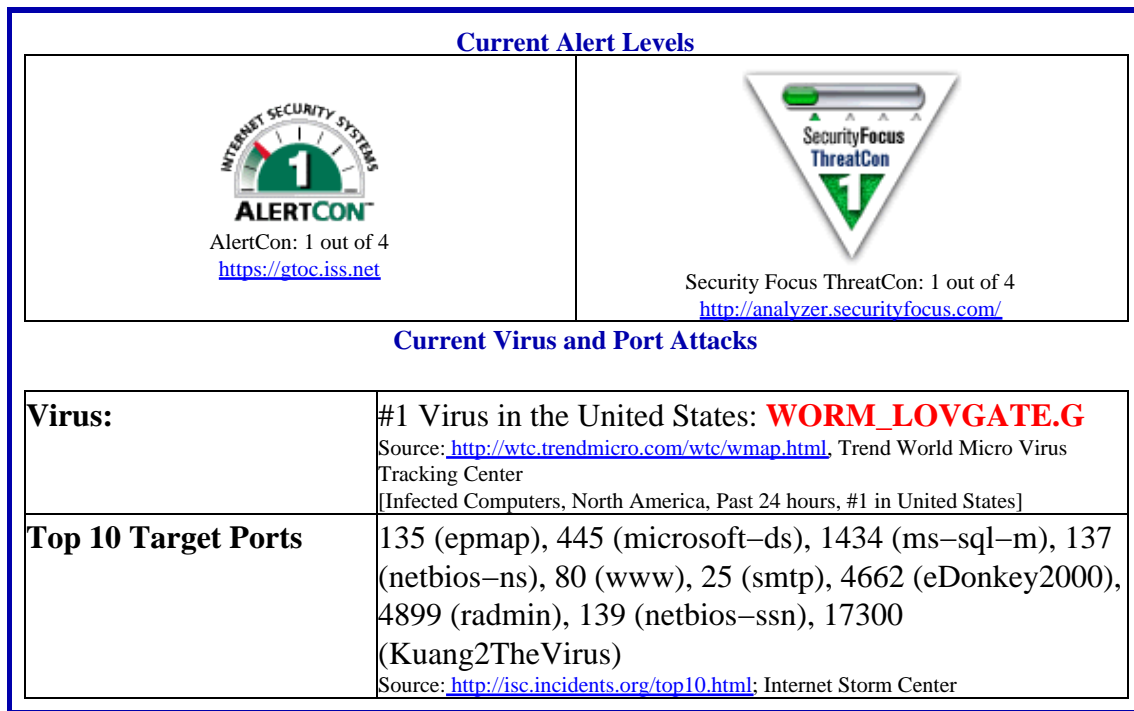# Information and Telecommunications Sector

24. *September 27, Washington Post* — **Juvenile arrested in Blaster case. Federal authorities announced Friday, September 26, that they have arrested a juvenile on charges of sending out a variant of the "Blaster" worm** that hit as many as 500,000 computers in August. The arrest was the second in the United States that targeted authors of altered versions of the Blaster worm, which led infected computers on an e–mail attack against Microsoft Web sites. The author of the Blaster worm itself has not been identified. In a statement **John McKay, U.S. attorney for the Western District of Washington, said that "computer hackers need to understand that they will be pursued and held accountable for malicious activity**, whether they be adults or juveniles." McKay also said his team is continuing its hunt for others involved with Blaster and its variants.
Source: http://www.washingtonpost.com/wp–dyn/articles/A7486–2003Sep2 6.html?referrer=email

25. *September 27, Reuters* — **IE holes lead to AIM, dial–up attacks.** Security holes in Microsoft's Internet Explorer (IE) are being exploited by hackers, computer experts cautioned Friday, September 26. Microsoft released a patch for the original hole about a month ago, said Stephen Toulouse of Microsoft, but is now looking into variations of that hole that the patch does not fix. **A hole in IE can hijack a running AOL Instant Messenger (AIM) account, change the password and send a message to the buddies list with a link to the malicious Website. Another attack sends computer users to Websites that change the computer's dial–up settings to an expensive long–distance phone number**, said security researcher Richard Smith. Victims are charged as much as $5 a minute instead of paying their normal Internet service fee, he said. **A third attack steers computer users to pay–per–click Websites, where the spam marketer gets paid each time someone goes to the Website**, said Drew Copley of eEye Digital Security. Computer users should apply patches, follow the workaround instructions, or change their settings in IE to prompt them before a Web site downloads programs that can execute on their own, Toulouse said.
Source: http://news.com.com/2100–7349_3–5083234.html

Internet Alert Dashboard

Current Alert Levels	
AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 445 (microsoft−ds), 1434 (ms−sql−m), 137 (netbios−ns), 80 (www), 25 (smtp), 4662 (eDonkey2000), 4899 (radmin), 139 (netbios−ssn), 17300 (Kuang2TheVirus) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

26. *September 30, The Advertiser (Australia)* — **New terror threat in Yemen. Yemeni authorities have alerted the United States to a potential new terrorist threat against foreign targets in Yemen, the State Department said on Monday. It called on U.S. citizens there to take "exceptional" security measures.** As a result of the new information, the U.S. embassy in Sanaa will hold a meeting of Americans in Yemen, al Qaeda leader Osama bin Laden's ancestral homeland, this week to discuss the new security situation, the department said. **The embassy issued a new warning to U.S. citizens in Yemen yesterday, telling them to redouble their already heightened security stance, particularly in and around areas frequented by foreigners in Sanaa and the port of Aden.** "The United States embassy has received new information from the Yemeni government regarding a potential new threat to foreign−affiliated and Yemeni targets," it said.
Source: http://www.theadvertiser.news.com.au/common/story_page/0,593 6,7416807%5E1702,00.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP
 To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer
 The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.